NETWORK INVESTIGATIONS TRACK

NIT480, Live Network Investigations (LNI)

Who Should Attend
DoD, federal law enforcement and technical support staff who require the ability to investigate live network traffic and environments.

Prerequisites
TT110 (INCH), RT120 (CIRC), NIT301 (NMC), NIT470 (ALA), FT210 (WFE-E) or FT215 (WFE-FTK) and one of the following: IT250 (FISE), IT260 (FIWE) or IT270 (FILE)

Duration
10 Days

Course Description
Trains students to conduct an intrusion investigation on large-scale, heterogeneous networks that are actively being compromised by unknown attackers. Students learn to assess the scope of a live, dynamic incident and apply a variety of investigative techniques while on-scene to identify the source, target, and methods of a network compromise through the use of free and commercially available tools.

Objectives
- Prepare for and assess the scope of a live dynamic network incident response
- Apply a variety of investigative techniques while on-scene
- Identify the source, methods used, and target of an intrusion
- Explain how to collect evidence in a live enterprise environment
- Perform an initial scope assessment with minimal data and constantly reassess scope based upon new findings
- Collect and analyze volatile data from multiple network devices and compromised computers
- Set up a system of network monitoring sensors and readjust the sensors during the course of the investigation
- Conduct a timely and efficient intrusion investigation on live servers with a variety of operating systems
- Use system entrenchment and monitoring techniques to further identify malicious activity on a known-compromised network segment

Topics Covered
Enterprise Networks and Intrusions
- Enterprise Architecture and Intrusion Methodology

Investigative Methodology
- Incident Response Lifecycle
- Incident Preparation, Case Management and Investigating Using the Scientific Method

LNI Detection and Analysis
- Witness Device Processing
- System Processing: Tools, Volatile Data Analysis and Direct Command Execution, Memory Dump, Live Imaging and Analysis,
- Network Monitoring
- Malicious Code Analysis

Continuation of the Incident Response Life Cycle
- Containment, Eradication, Recovery and Post-Incident Activities
- Interim and Final Reports

NETWORK INVESTIGATIONS TRACK

Preparation

To prepare for this course, we recommend the following review, reading, or research:

- Review the *Introduction to Networks and Computer Hardware* (INCH) course book, paying special attention to:
  - Operating Systems, specifically MS Windows Operating Systems Basics
  - Windows XP Command Line
  - Windows 7, Internet Explorer 8
  - Windows Registry
  - Basic networks (including the OSI Model), Network Connectivity, Configuration (including ports), Protocols and Devices
  - IP Addresses, Subnets and Network Security (specifically Anti-virus Software, Firewalls, IDS, Logs)
- Review the *Computer Incident Responders Course* (CIRC) course book, paying special attention to:
  - OSI Layer Functions and Physical Assessment
  - Witness Devices – Networks and Witness Devices, Switches, Firewalls, Routers, Sniffers and Intrusion Detection Systems, Remote Logging
  - Windows 2003 Server Information Collection
- Review the *Windows Forensic Examinations* (WFE) course book, paying special attention to:
  - Getting Started – The Laboratory Request and Forensic Reporting
  - Beginning a New Case with EnCase – Beginning a case, Digital Media Validation, The EnCase GUI, Bookmarking
  - Forensic Analysis Basics – Windows and the Windows Registry
  - Initial Forensic Analysis with EnCase – Malicious Code Scanning, File Signature Analysis, Hash Analysis, Keyword Searching
  - Using Automated Tools – Filters and Conditions, Date Searching
  - File Level Analysis – Web Related Evidence
- Review the *Forensics and Intrusions in a Windows Environment* (FIWE) course book, paying special attention to:
  - Network Architecture Basics, Wireshark, Network and Application Protocol Analysis
  - Identification of Intrusions – Computer Intrusions, Reconnaissance (specifically Goals and Strategies), Attacks (specifically Goals and Strategies), Entrenchment (specifically Goals and Strategies), Abuse (specifically Goals and Strategies)
  - System Preparation and Forensic Analysis – Windows OS, Fundamentals of Windows Artifact Analysis, Forensic System Setup (specifically introduction to EnCase), Initial Case Processing, Analyzing First Responder Data, File System Searching and Filtering, Windows Registry Analysis, System Log Analysis
  - Fundamentals of Network Artifact Analysis, Network Device Artifact Analysis, Network Traffic Capture Analysis
- Professional network security Web Sites and Network log analysis Web sites
- Review CCNA, CISSP, or other system administration certification study material

These topics are covered in DCITA courses you may have attended previously and can also be found on the dcita.edu portal (https://www.dcita.edu), the internet, at Books 24/7, in your organization's technical library or at the public library. Instructions for D-Prep on the dcita.edu portal: log in. Under Online Courses (INCH/CIRC/WFE/FIWE), select DPrep Training; Course Name; Sort by Name Ascending.

LNI Grading Policy

Student progress is monitored through instructor observation during lecture, discussion and practical exercises as well as Knowledge and Performance Tests. Minimum passing score on all DCITA tests is 70%.